



INSTITUTE FOR DEFENSE ANALYSES

## **Data to Decisions—Terminate, Tolerate, Transfer, or Treat**

Laura A. Odell

25 July 2016

Approved for public  
release; distribution is  
unlimited.

IDA Non-Standard  
NS D-8094

Log: H 2016-000881

Copy

INSTITUTE FOR DEFENSE  
ANALYSES  
4850 Mark Center Drive  
Alexandria, Virginia 22311-1882



*The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.*

#### About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task BK-5-3889, "Creating an Affordable Strategy for Policy Issuance and Buying Power for the DoD CIO," Office of the Secretary of Defense, Chief Information Officer. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

#### Copyright Notice

© 2016 Institute for Defense Analyses  
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [Jun 2013].

# IDA Data to Decisions—Terminate, Tolerate, Transfer, or Treat

The Department of Defense (DoD) is increasingly concerned that the loss of sensitive data to our adversaries is eroding the competitive advantage of the United States. This sensitive data includes business proprietary information on key programs of record and infrastructure, including government documents at the Federal and State levels that describe gaps in and limitations of our national assets. This loss of data compromises the effectiveness of our readiness for defense of the nation, and it minimizes the investments we have made to build advantages into our offensive and defensive capabilities—needed for protection in the event of an attack. The customary kinetic thin line, a basic level of survivability and resiliency to protect our most critical assets at the Federal level, may not be broad enough to include the full scope of issues that arise as adversaries seek to compromise our key defenses and national physical assets through breaches of our networks and other electronically initiated means.

For these reasons, the DoD Office of the Chief Information Officer (CIO) is beginning to share knowledge and create templates that the States and territories can leverage nationally. The Institute for Defense Analyses (IDA) assisted the DoD CIO in formalizing a proof of concept for cyber initiatives and developed frameworks for operationalizing the data and intelligence produced across State structures and organizations. While States are pursuing the resolution of cyber issues across many fronts, a significant gap remains between the ability to gather and share information and intelligence and the mitigation of breaches that have already occurred.

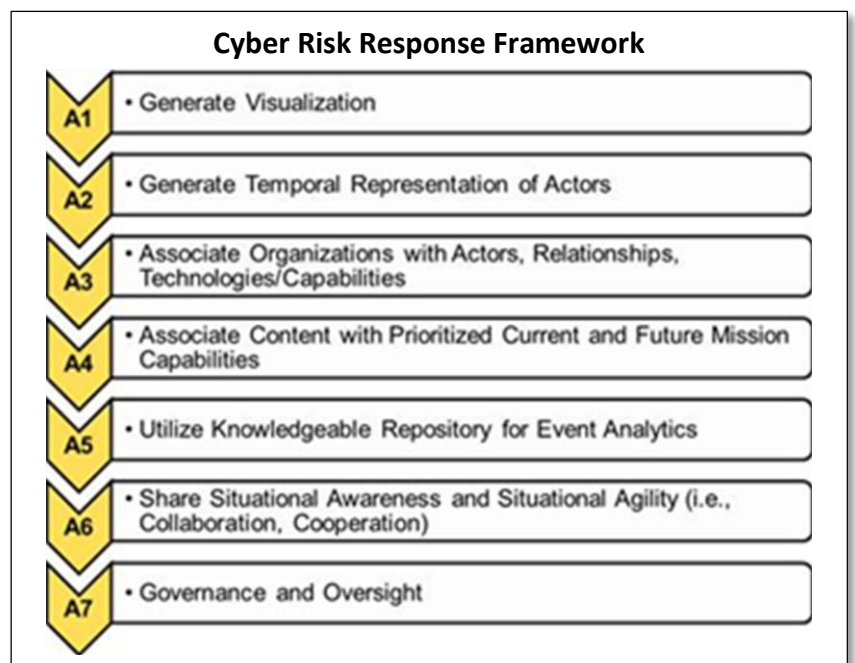
In lieu of a compliance-based cybersecurity model focused on the state of networks, malware, and patching, a risk-based cybersecurity decision model that enables a predictive capability to respond to impending cyber-attacks is needed. Operationalizing the analysis of data, information, and intelligence from disparate sources across multiple service sectors to provide a common operating picture and decision framework for State governments, law enforcement, emergency services, the Department of

Homeland Security, the National Guard, industry, international stakeholder “partners,” and others must begin now.

**Data to Decision.** If an adversary has the technology or capability to do harm, then an *incentive* (desire to invest time, resources) to use the technology/capability is required to effect plausibility of a cyber incident. That is, even if an adversary has the means to do harm, there may not be an incentive to do so. Determining the appropriate investment necessary to address high priority *impact* events is a key consideration given fiscal constraints, and plausibility includes both the technology involved and the motive to use it.

The framework below provides context and a common understanding for cyber decision-making to help Federal and State leaders operationalize intelligence and information:

1. *Generate visualization* – Geospatial representation is important to consider when dealing with actors—but it can be misleading. Hackers for hire and other third-party actors may be state-sponsored and not physically located at the origination point of the attack. Although the association of location to content may be manipulated, every actor has signatures that machines can identify.
2. *Generate temporal representation of actors* – In



cyberspace, time is both relevant and irrelevant. It is irrelevant because incidents only occur when there is a congruence of sufficient intent and capability (i.e., Bash was a vulnerability for over twenty years but only became relevant when hackers sought to exploit it). However, domestic and international triggers/hooks (i.e., lifting sanctions, which puts more funding into play to hire third-party actors to commit cyber-attacks) may be an indicator (forcing function) in predicting an attack. The ability to anticipate/control the progression of events to maximize the opportunity to observe the adversary and know the time when they are most prepared to act is critical.

3. *Associate Organizations with Actors, Relationships, Technologies/Capabilities* – Not all cyber risk is high-impact. Intent and capabilities should put these in the context of a wider knowledge of actors and relationships (i.e., nation-states, corporate states, and criminal organizations) to improve insight into the threat.
4. *Associate Content with Prioritized and Future Mission Capabilities* – National assets should be prioritized based on their potential impact on our nation. Responses to threats or data losses should be weighed in the context of their importance to the overall mission outcome.
5. *Utilize Knowledgebase Repository for Event Ana-*

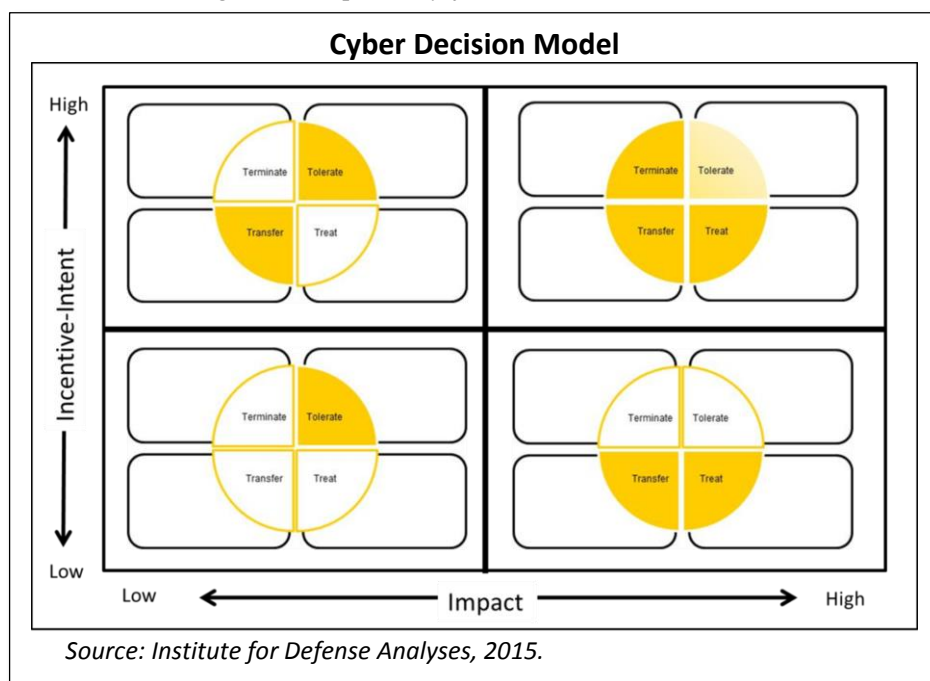
*lytics* – Federal and State governments should expand their sources of information to include international actors, non-state actors, event histories, social media, and episodic behaviors. These sources could assist in contextualizing and filling gaps in knowledge. The United States should begin to leverage non-traditional data sources to better protect and defend against cyber intrusions and attacks.

6. *Share Situational Awareness and Situational Agility* – Awareness is important, but alone, it is not enough. The accelerated nature of many cyber-attacks requires a readiness to act and commitment to a rapid response with already established trusted systems and communities of interest.
7. *Governance and Oversight* – As Federal and State governments seek to develop and expand automated courses of actions and thresholds, the global community is a key resource in developing a better understanding of the cyber risk (i.e., agreements across shared borders with Canada and the Soo Locks in the State of Michigan).

***The Decision to Terminate, Tolerate, Transfer, or Treat Risk.*** A cyber vulnerabilities risk management approach should offer decision makers several choices when assets are assessed as being vulnerable to or experiencing cyber exploitation. Rather than

simply accepting risk or investing in a mitigation action, using a framework based on the choices of Terminate, Tolerate, Transfer, and Treat is more appropriate for managing the dynamic and accelerating pace of cyber intrusion incidents. These choices present both opportunities and consequences.

The framework ensures that a decision maker is not limited to the more traditional yes/no and if/then/else decision construct to afford a deeper understanding of what could be gained or lost. The framework applies equally well to early invest-



ments and fully operational systems. Specific considerations for fully operational systems include the following.

#### **Terminate – Opportunities and Consequences:**

- Terminating a capability/technology may notify the adversary that he is **DISCOVERED**.
- There is no longer an opportunity to observe adversary targets and techniques.
- Although the incident is no longer a degradation to the system or environment, the capability/technology is lost and may have to be replaced if there are no substitutes.

#### **Tolerate – Opportunities and Consequences:**

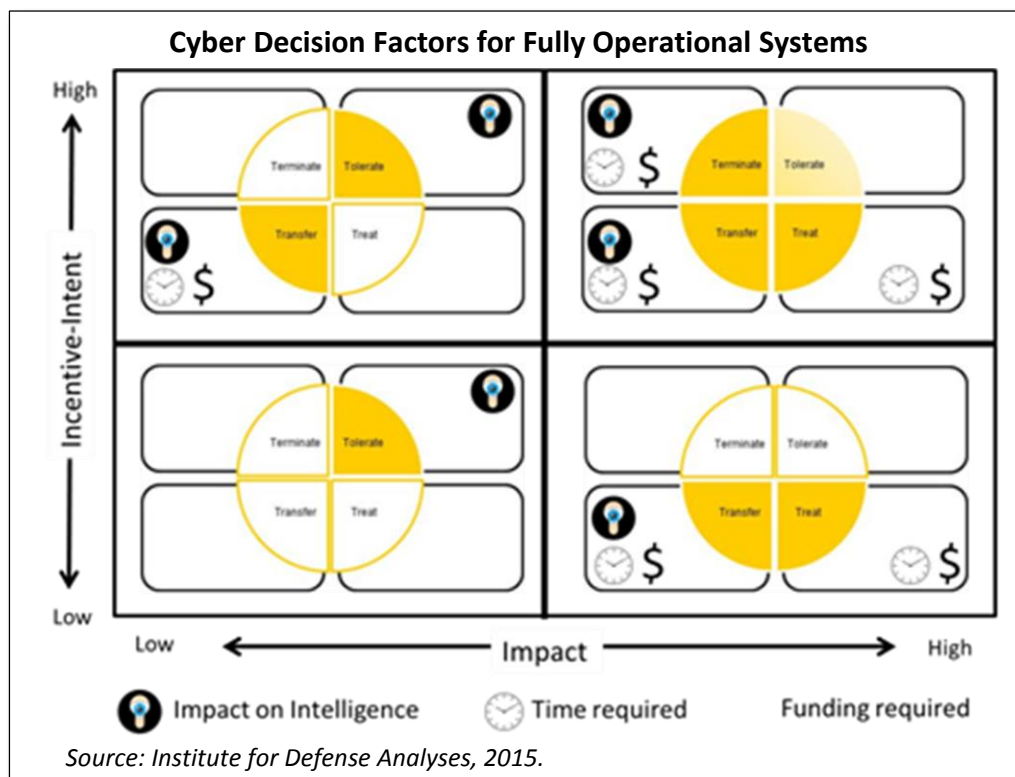
- Avoids investment in lesser priorities deemed low impact.
- Allows time to develop a more informed understanding of the adversary and defend against future attacks afforded by the opportunity to observe.
- However, observation takes time and resources.
- Degradation of current capability continues.

#### **Transfer – Opportunities and Consequences:**

- Requires a surgical knowledge of what alternatives are technically available and what is feasible.
- Funding and other resources may be required.
- May need cooperation and collaboration from stakeholders (sometimes difficult to coordinate) outside an organization or country.
- Time is needed for correction, socialization, and application of solution.
- May afford an opportunity to promote a solution from a singular platform to an enterprise-level application.

#### **Treat – Opportunities and Consequences:**

- Time and funding are required to treat and mitigate a risk.
- Know-how or knowledge is required that may not be contained in the original solution.
- There may be an opportunity to manipulate or create a false provenance or misinform the adversary (i.e., in cases of exfiltration).
- New opportunity to build in defensive design.



A decision to terminate, tolerate, transfer, or treat risk must include at a minimum: (1) what is known about (intelligence) the adversaries' current capabilities, (2) the incentive of the adversary to use those capabilities against a target of importance, and (3) an assessment of the impact level of the asset (priority to the organization).

*Note: This paper is a companion document to IDA publication number NS D-8008, A State Cyber Hub Operations Framework, dated June 2016, approved for public release; unlimited distribution.*



REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. <b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b>					
1. REPORT DATE (DD-MM-YY) 25-07-16		2. REPORT TYPE Non-Standard		3. DATES COVERED (From – To)	
4. TITLE AND SUBTITLE Data to Decisions—Terminate, Tolerate, Transfer, or Treat				5a. CONTRACT NUMBER HQ0034-14-D-0001	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBERS	
6. AUTHOR(S) Laura A. Odell				5d. PROJECT NUMBER BK-5-3889	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882				8. PERFORMING ORGANIZATION REPORT NUMBER NS D-8094 H 2016-000881	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Kevin Garrison Principal Director/Director Analytics, Office of the Secretary of Defense, Chief Information Officer The Pentagon, Rm. 3B1056				10. SPONSOR'S / MONITOR'S ACRONYM OSD CIO	
				11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES Project Leader: Laura A. Odell					
14. ABSTRACT The Department of Defense (DoD) is increasingly concerned that the loss of sensitive data to our adversaries is eroding the competitive advantage of the United States. A framework is needed for building the context and common understanding for cyber decision-making. Federal and State leaders must operationalize intelligence (Incentive and Impact) and information.					
15. SUBJECT TERMS Data to Decisions, Cyber Hub, Terminate, Tolerate, Transfer, Treat, Incentive/Impact framework					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT  Unlimited	18. NUMBER OF PAGES  3	19a. NAME OF RESPONSIBLE PERSON Kevin Garrison
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (Include Area Code) 703-614-2778

